DoD Trusted Defense Systems

Ms. Kristen Baldwin
Director, Systems Analysis
DDR&E/Systems Engineering
“Software Assurance Forum”
28 September 2010

Approach to Trusted Defense Systems

Buying with Confidence

Building with Integrity

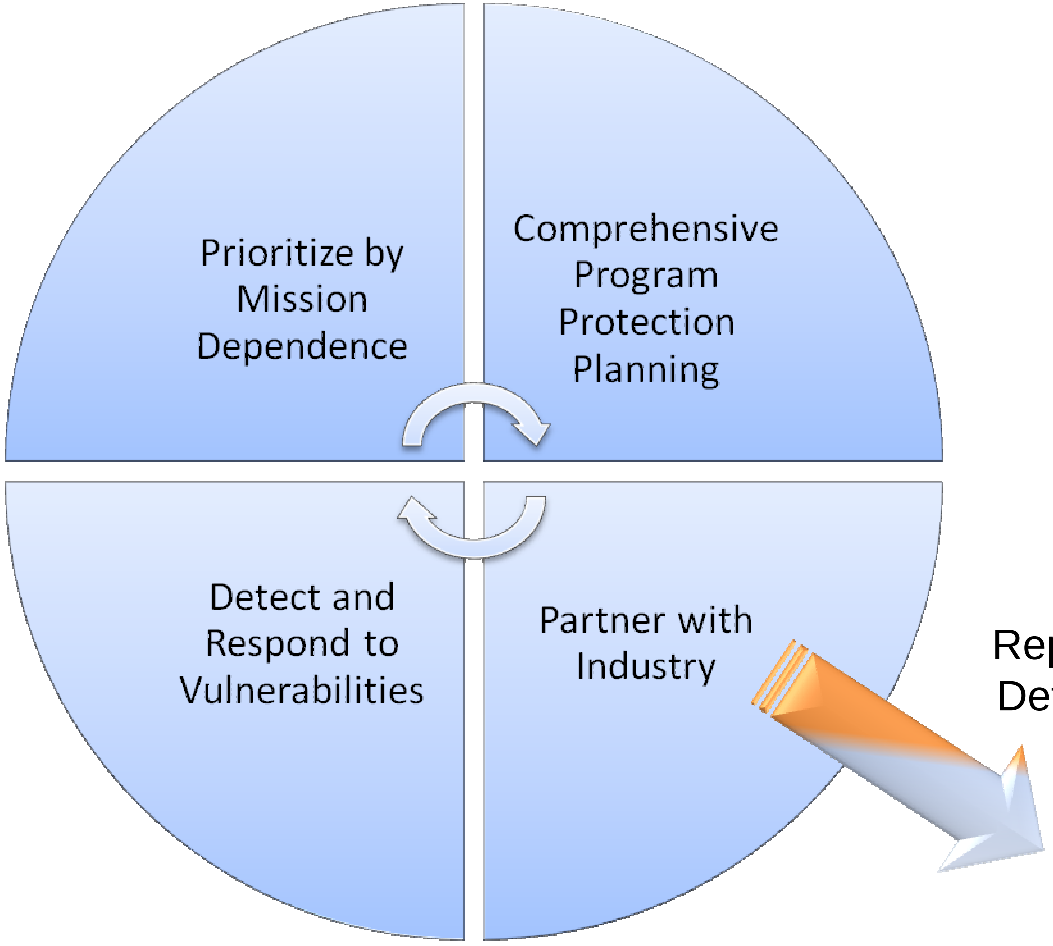
Ensuring Horizontal Protection

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Trusted Defense Systems Strategy

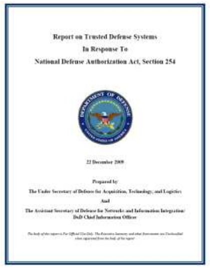
Drivers/Enablers

- National Cybersecurity Strategies
- Congressional Interest
- DoD Policy and Directives
- Globalization Challenges
- Increasing System Complexity


Prioritize by Mission Dependence
Comprehensive Program Protection Planning
Detect and Respond to Vulnerabilities
Partner with Industry

Delivering Trusted Systems

Report on Trusted Defense Systems



Report on Trusted Defense Systems
In Response To
National Defense Authorization Act, Section 254

22 December 2009

Prepared by
The Under Secretary of Defense for Acquisition, Technology, and Logistics
And
The Assistant Secretary of Defense for Networks and Information Integration/
DoD Chief Information Officer

The body of this report is For Official Use Only. The Executive Summary and other Enclosures are Unclassified when separated from the body of the report

USD(AT&L)
ASD(NII)/DoD CIO

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Increased Priority for Program Protection

- ***Threats*: Nation-state, terrorist, criminal, rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities*: All systems, networks, applications**
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences*: Stolen critical data & technology; corruption, denial of critical warfighting functionality**

Today's acquisition environment drives the increased emphasis:

Then		Now
Standalone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers

Major Efforts being executed by DDRE/SE

- **Implementing 5200.39 and 5000.02 Program Protection Policy**
  - Review/Coordination of PPPs for ACAT I programs
  - Program protection assessment methodology
  - Guidance and best practice countermeasures, education and training, industry outreach, to assist programs with CPI identification and protection
- **Supply Chain Risk Management**
  - Procedures, capability to utilize threat information in acquisition
  - Commercial standards for secure components (ISO/IEC, The Open Group)
- **Horizontal Protection Procedures**
  - Acquisition Security Database (ASDB) oversight and implementation
- **Advancing the practice: Systems Security Engineering**
  - SERC Research Topic – “Security Engineering”
  - INCOSE Working Group on Systems Security Engineering
  - DoD/NSA Criticality Analysis Working Group
- **DoD Anti-Tamper Executive Agent**
  - Anti-Tamper IPT, AT policy, guidance advocate
  - Legislative Proposal – Defense Exportability Fund Pilot Program
- **Countering Counterfeits Tiger Team**
  - Lifecycle strategy to reduce counterfeits, especially microelectronics

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Challenges Being Addressed

- Policy and guidance for security is not streamlined
- There is a lack of useful methods, processes and tools for acquirers and developers
- Criticality is usually identified too late to budget and implement protection
- Horizontal protection process is insufficiently defined
- Lack of consistent method for measuring cost and success of “protection”
- Intelligence data is not available to programs for risk awareness
- Security not typically identified as an operational requirement, and is therefore lower priority

Data Source: GAO report, white papers, military service feedback

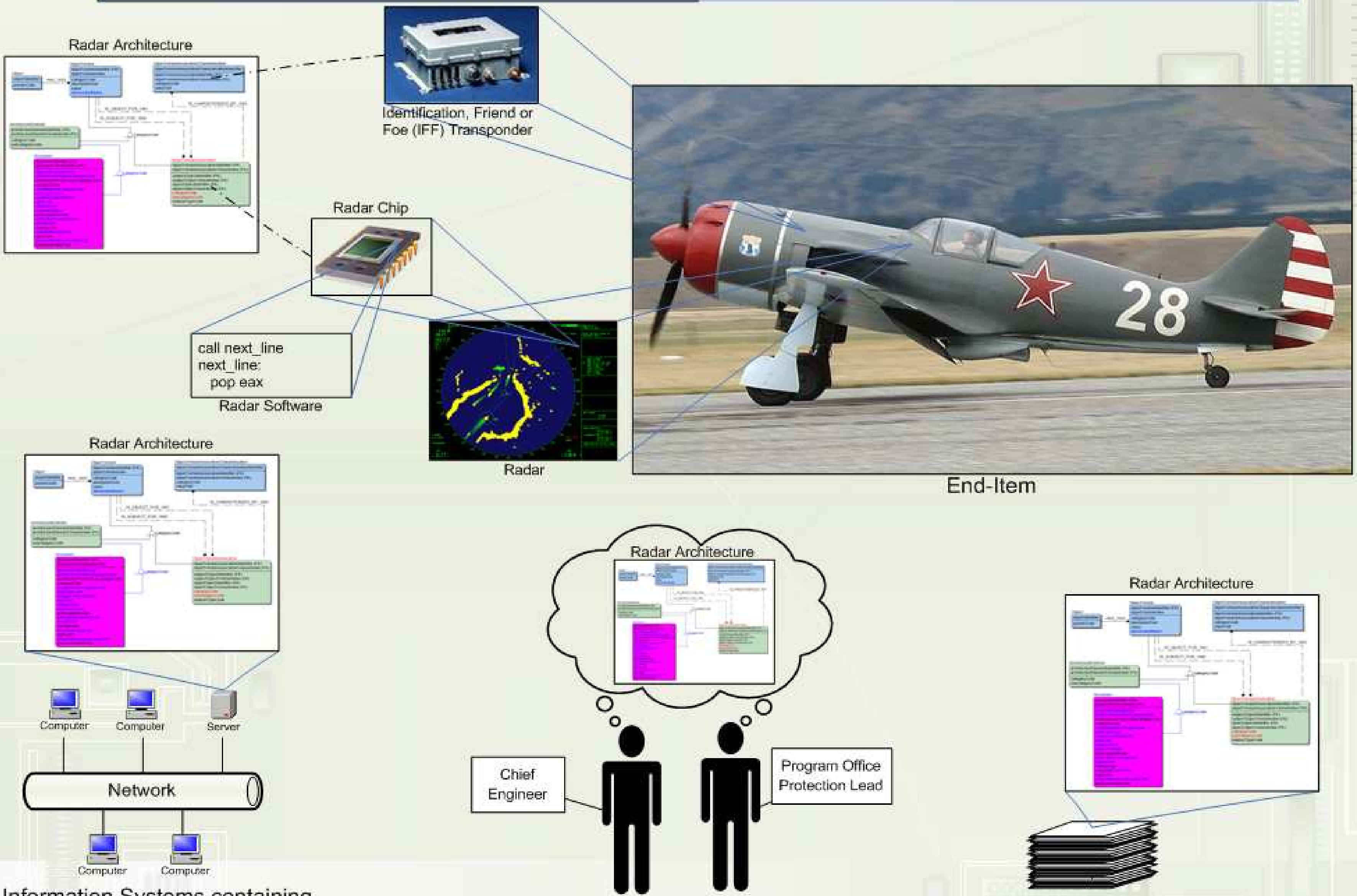
Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Program Protection Policy

- **DoD Policy: DODI 5200.39 “Critical Program Information Protection Within the DoD”**
  - Provide uncompromised and secure military systems to the warfighter by
    - performing comprehensive protection of CPI
    - through the integrated and synchronized application of CI, Intelligence, Security, systems engineering, and other defensive countermeasures to mitigate risk…
  - “CPI. Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness;
    - Includes **information** about applications, capabilities, processes, and end-items.
    - Includes **elements or components** critical to a military system or network mission effectiveness.
    - Includes **technology** that would reduce the US technological advantage if it came under foreign control…”

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

What are the formats of CPI?



Radar Architecture

Identification, Friend or Foe (IFF) Transponder

Radar Chip

```
call next_line
next_line:
  pop eax
```

Radar Software

Radar

End-Item

Radar Architecture

Computer

Computer

Server

Network

Computer

Computer

Information Systems containing information about the aircraft

Radar Architecture

Chief Engineer

Program Office Protection Lead

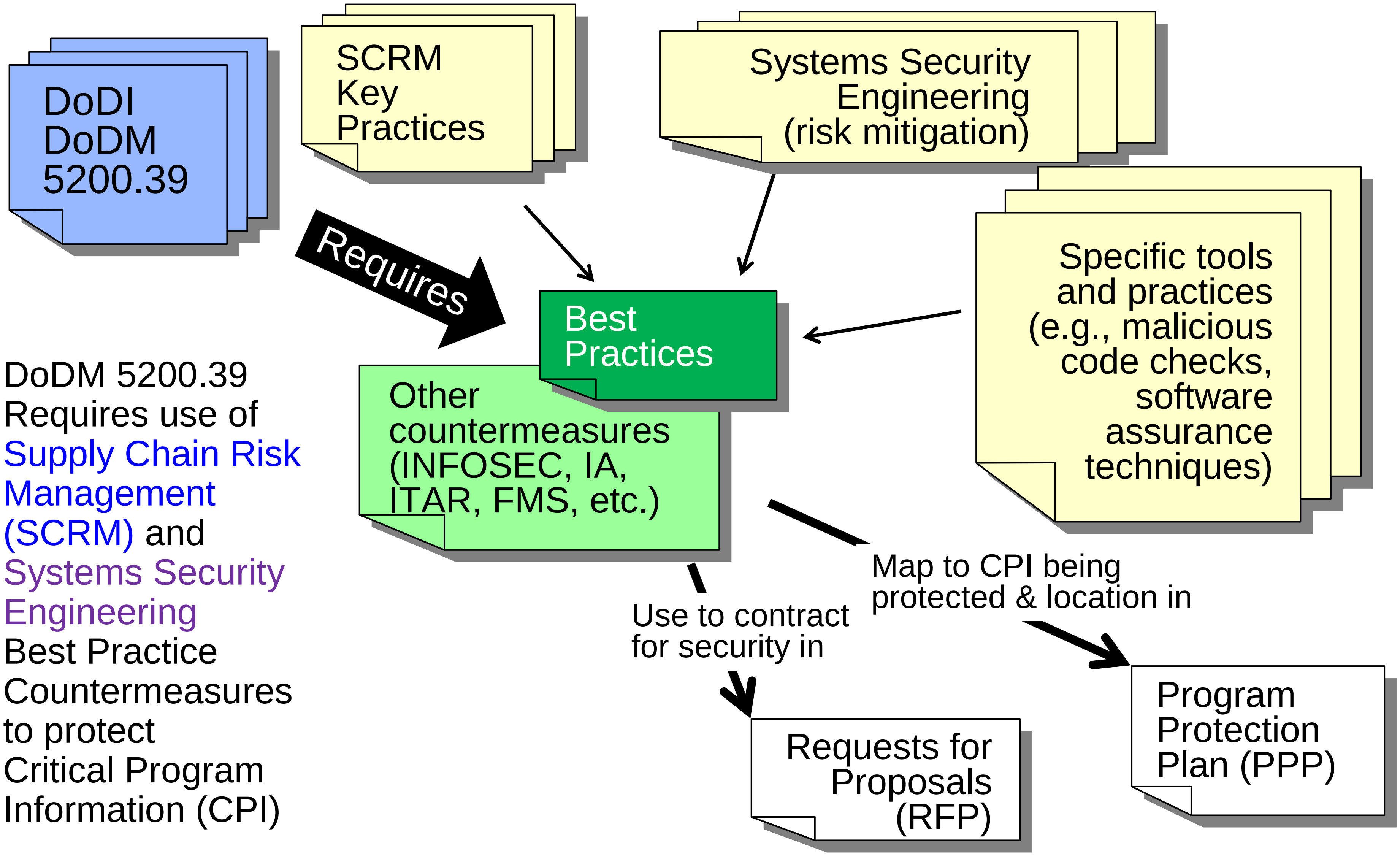
People with knowledge of the aircraft

Radar Architecture

Hard copy information about the aircraft

Notional Diagram – Does not illustrate actual locations of CPI or components of any aircraft

Multifaceted Approach to Program Protection



DoDM 5200.39
Requires use of

- ✶ Supply Chain Risk Management (SCRM) and
- ✶ Systems Security Engineering

Best Practice Countermeasures to protect Critical Program Information (CPI)

Systems Security Engineering

- **Systems Security Engineering Definition:**
  - An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities

    (MIL-HDBK-1785: System Security Engineering Program Management Requirements)

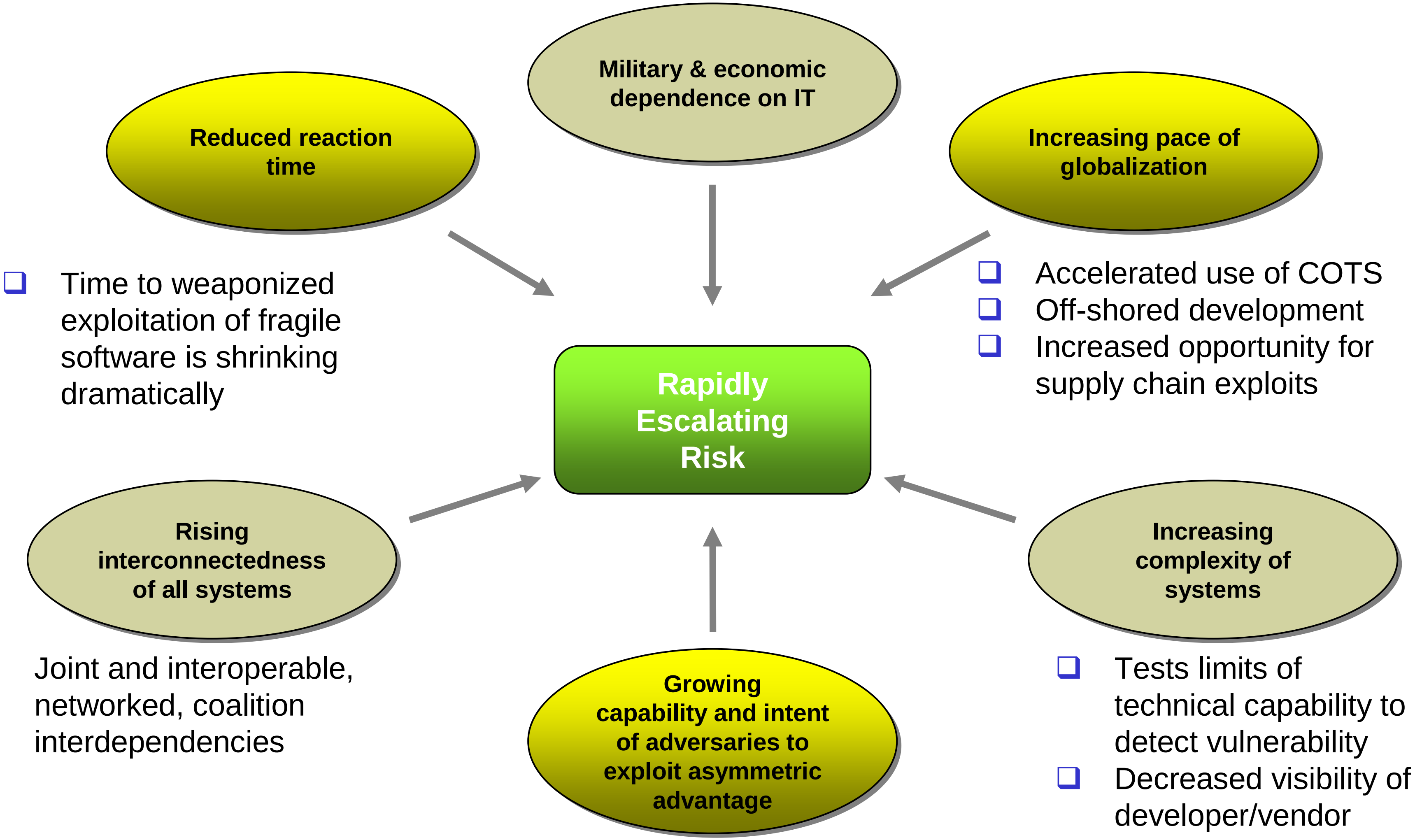
Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Systems Security Engineering (SSE): Early Engineering Emphasis

- **Identify components that need protection**
  - Perform criticality analysis based on mission context and system function
    - Evaluate CONOPS, threat information, notional system architecture to identify critical components (hardware, software and firmware)
    - Identify rationale for inclusion or exclusion from candidate CPI list
  - Perform trade-offs of design concepts and potential countermeasures to minimize vulnerabilities, weaknesses, and implementation costs
- **Establish Systems Security Engineering Criteria**
  - Ensure preferred concept has preliminary level security requirements derived from candidate CPI countermeasures
  - Ensure system security is addressed as part of Systems Engineering Technical Reviews
- **We have begun to apply these practices with major acquisition programs**

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Factors Accelerating Program Protection Complexities



Military & economic dependence on IT

Reduced reaction time

- Time to weaponized exploitation of fragile software is shrinking dramatically

Increasing pace of globalization

- Accelerated use of COTS
- Off-shored development
- Increased opportunity for supply chain exploits

Rapidly Escalating Risk

Rising interconnectedness of all systems

- Joint and interoperable, networked, coalition interdependencies

Growing capability and intent of adversaries to exploit asymmetric advantage

Increasing complexity of systems

- Tests limits of technical capability to detect vulnerability
- Decreased visibility of developer/vendor performers

DoD is banking on the integrity of software/hardware/IT

Commercial Market Factors Voiced by Industry

- Industry is building IT commodity products for a global market, of which US DoD share is ~2%-4%, varies by sector.
- The commercial market drivers for IT far outweigh DoD Supply Chain Risk Management (SCRM), Information Assurance (IA), and Systems Assurance (SA) concerns (it is what it is)
- DoD is increasingly (compelled by technical cost and schedule factors) leveraging commercial technology and products in building its PORs
- Industry efforts to build one-off products to security specs, e.g. NIST, Common Criteria, Evaluated Products Lists, ISO 9000, etc add too much cost, and result in late-to-need, unfriendly consumer products and limited sales

How are we engaging with Industry

- **We have turned to The Open Group**
  - – based upon their **membership** (thousands of companies),
  - – **processes** (they defined UNIX and interoperability),
  - – **consortia** (they already work these same issues for financial, aerospace, and international security sectors).
- **To facilitate a discussion of secure product development**
- **We are interested to take this discussion further**

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

The Open Group

Trusted Technology Provider Framework (TTPF)

Purpose

Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices that can mitigate vulnerabilities which could lead to exploitation and malicious threats to product integrity.

Objectives

- Identify product assurance practices that should be expected from all commercial technology vendors based on the baseline best practices of leading trusted commercial technology suppliers
- Help establish expectations for global government and commercial customers when seeking to identify a trusted technology supplier
- Leverage existing globally recognized information assurance practices and standards
- Share with commercial technology consumers secure manufacturing and trustworthy technology supplier best practices
- Harmonize language used to describe best practices

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Summary

- **Buying with Confidence**
  - Open Group engagement to develop secure commercial product standards
  - Technology supply chain security standard through ISO
  - Supply Chain Risk Mitigation
  - Countering Counterfeits Tiger Team
  - Object Management Group software assurance frameworks
- **Building with Integrity**
  - NDIA System Assurance Guidebook, adopted by NATO Standardization Agency
  - ISO 15026: Standard for Systems and Software Assurance
  - Criticality Analysis Working Group
  - Systems Security Engineering research roadmap
  - DHS Software Assurance
- **Ensuring Horizontal Protection**
  - DoD-wide Critical Program Information identification process
  - DFARS for safeguarding unclassified DoD information on DIB networks
  - Acquisition Security Database adoption and implementation

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies

Discussion

Threading the Needle
~Assurance through Engineering~
Part 1

- **Adapting to a changing environment**
  - We live in a dangerous world
  - Protection of current and future defense information is critical
  - Use of commercial technology provides significant benefits
  - Commercial technology is increasingly a global enterprise effort
  - We are designing our systems and networks to leverage commercial products where possible, and Mil Spec pieces, only where needed
  - The bottom line is higher assurance, within cost and schedule

Threading the Needle
~Assurance through Engineering~
Part 2

- **Achieving assurance through Program Protection Planning**
  - The DoD response to Globalization Challenges includes renewed emphasis on Program Protection Planning (PPP)
  - PPP requires rigorous systems engineering review to identify what to protect and cost-effective threat mitigations
  - Taken together we are invigorating Systems Security Engineering (SSE)
  - We are working across industry to encourage more trustworthy commercial products

Distribution Statement A – Cleared for public release by OSR on 27 Sep 2010, SR Case # 10-S-3388 applies